REMARKS

Claims 1-23 are pending in this application, all of which stand finally rejected. Claims 1-4 and 7-8 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Published Application No. 2004/0091114 (Carter). Claims 5, 9-10, 12, 14-15, 18, 20, and 23 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Carter in view of U.S. Published Application No. 2003/0188179 (Challenger). Claims 6, 19, and 22 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Carter in view of Challenger and in further view of U.S. Published Application No. 2004/0190714 (Masui). Claims 11, 13, 16, 17, and 21 have been rejected as being unpatentable over Carter and Challenger in view of a modification proposed by the Examiner that the Examiner admits is not found in either reference. Claims 20-22 have been rejected under 35 U.S.C. § 101. Following entry of the amendment, claims 1, 6, 12, 20, 21, 22, and 23 will have been amended, and claims 4 and 5 will have been canceled.

Section 101 Rejection

Claims 20-22 have been amended to recite a "computer-readable storage medium." In view of this amendment, applicants request that the section 101 rejection be reconsidered and withdrawn.

Section 102/103 Rejections

Independent claims 1, 9, 14, 20, and 23, as presently written, each recite features relating to the unavailability of a key across reboots. While the claims are not identical in either scope, language, or substance, each of these independent claims recites, in effect, that the key is used for decryption of data contained in a paging file, and that the key either is lost if the machine is rebooted (claims 9 and 23), or that the key does not persist across reboots (claims 1, 14, and 20). These features are not taught in the references as applied.

The Examiner acknowledges (Office Action, p. 5) that Carter does not teach that a key is stored in a manner that causes the session key to become unavailable or lost after a boot, and instead relies solely on Challenger for this feature.

The Examiner's reliance on Challenger is misplaced. Challenger (see paragraphs 0054-0058) describes a system in which the key that is used to decrypt a file system can be exported for use for only a very short period of time during the machine boot sequence. In particular, the machine maintains certain registers called PCRs, and the PCRs must all be at specific values in order to allow export of the key. The PCRs remain at the right values for a very short period of time, thereby reducing the amount of time that the key is available to be exported. The short amount of time that the key is available for export is said to protect the key from being used inappropriately.

However, what the Examiner overlooks is that the key that is exported in Challenger is the same key each time the machine is booted. Thus, the key in Challenger is not lost across boots, and does not fail to be persisted across boots, as in the claims of the present application. This is because Challenger's key is being used to decrypt a file system that stores long-term files, and these files would become unusable if the key were lost (or not persisted) across boots.

However, making a file unusable is precisely a point of the technique recited in the claims. While the claims do not import limitations from the specification, the specification provides useful background on the claim features, which is reproduced below for the Examiner's convenience:

> [0034] … The session key is preferably not stored in a manner that would persist the key across boots; thus, encrypted paging file data that was generated in one boot cannot be decrypted beyond the current session, thereby protecting the security of that data. (For example, if the hard disk is removed from the computer and stole, the disk should not contain a copy of the session key that would allow the paging file data to be decrypted when the disk is installed on another machine.)

It should be understood that the file that the key is used to decrypt is a paging file – a file that stores ephemeral data of the type that would normally be kept in memory. As explained in the application (paragraph 0006): "Paging files are different from ordinary files in the sense that paging files are temporary repositories for data that is meaningful only in the context of a

single instantiation of a computing environment (e.g., between boots of a machine)." Since the contents of the computer's memory needs to be repopulated across boots, memory data from the last boot is not needed after the machine has been rebooted, and it is desirable, from a security and privacy standpoint, for this data to become unavailable after the machine is rebooted. Since a paging file stores this type of temporary memory data, the present claims cause the decryption key for the paging file to be lost, or not persisted, across boots of the machine.

Not so in Challenger, where file system data to be decrypted is long-term data that needs to be available across boots. Thus, while Challenger takes steps to resist unauthorized capture of the key, it still produces the same key across boots. Challenger must produce the same key, since the same data needs to be decrypted across boots. By contrast, in the present claims, the key is lost, or not persisted, across boots, thereby preventing the paging file data from being decrypted.

Since Challenger is storing long-term data that needs to be decrypted across boots, and the present claims call for the decryption key to be lost, or not persisted, across boots, Challenger can be said to *teach away* from the present claims. In view of this teaching away, the claims are not obvious over Challenger. Of course, references that teach away from their combination cannot be combined to form an obviousness rejection. MPEP 2145(X)(C)(2).

Turning to the language of the claims, each of the independent claims calls, in some manner, for a key to be used for encryption and/or decryption of the paging file or of information stored therein:

- Claim 1: "…the session key being further needed for subsequent decryption of the encrypted data …"

- Claim 9: "…said key being required to decrypt information contained in said paging file …"

- Claim 14: "…performs encryption and decryption operations on said data using a key …"

- Claim 20: "… encrypting the received data with a session key prior to storing said data in the paging file …"

- Claim 23: " … said key being required to decrypt information contained in said paging file …"

Furthermore, each of these claims calls for a reboot of the machine to cause the key to be lost (9 and 23), or for the key not to be persisted across reboots (1, 14, and 20). For the reasons discussed above, these features are contrary to Challenger, because Challenger does persist the key across boots of the machine, and requires a persistent key to decrypt long-term files. (As noted above, the Examiner admits that the feature of a key that is lost when a machine is rebooted is not found in Carter.

For these reasons, applicants submit that the independent claims, as presently written, are not obvious over the combination of Carter and Challenger, and request that the rejection of these claims be reconsidered and withdrawn.

Moreover, dependent claims 11, 16, and 21 each call for reserving a block of memory prior to generation of the key, where the block of memory is used either as a workspace (claims 11, 16, and 21) or a buffer (claim 21). The Examiner does not cite any reference for this feature, and acknowledges that this feature is not found in either Carter or Challenger. Rather, the Examiner simply asserts – without citing a reference, and without taking official notice of any fact – that it would be obvious over the combination of Carter and Challenger to add this feature. Applicants submit that the Examiner misunderstands this significance of this feature.

Claims 11, 16, and 21 do not merely call for reserving a block of memory, but rather call for doing so prior to the generation of the key. This block of memory may be used as a workspace for the encryption component itself: since there is a risk that portions of the components might be paged to disk before the pagefile encryption key has been created, reserving a block of memory, for use as a buffer or workspace, before the encryption key has even been created mitigates this risk.

It should be noted that the Examiner's explanation of what would motivate one to alter Carter and Challenger is incorrect, and has nothing to do with the actual feature as claimed, or as described in the application. In particular, the Examiner states: "Since the encryption key is stored in a particular block of the volatile memory (instead of scattering over different blocks), this make [sic] the encryption key being [sic] easy to control and protect." However, there is nothing in claims 11, 16, or 21 that requires the encryption key to be stored in the reserved block of memory, so it is unclear what relevance the Examiner's comment has. There is nothing in Carter or Challenger that would motivate one to reserve a

block of memory as a buffer or workspace, and, in particular, to do so at a time that is prior to creation of the encryption key.

The foregoing comments provide additional reasons why dependent claims 11, 16, and 21 are patentable over the applied references.

Finally, as to claims 6, 19, and 22, the Examiner relies on Masui for its alleged teaching of avoiding persistent storage, or disk storage, of an encryption key. However, the applied portion of Masui teaches or suggests no such thing. Paragraph 0014 of Masui says that an encryption key can be stored in volatile memory, but there is nothing in this paragraph that teaches or suggests that the key could not also be stored persistently or on disk. It is possible to store a key in volatile memory, and also to store the same key persistently or on disk. Since claims 6, 19, and 22 call for the key not to be stored persistently (claim 6) or not to be stored on disk (claims 19 and 22), this feature cannot be inferred from Masui.

The foregoing comments provide additional reasons why dependent claims 6, 19, and 22 are patentable over the applied art.

No new matter

Claim 1 has been amended by incorporating the subject matter of now-canceled claims 4 and 5, and also by altering its language in a manner supported at least by paragraph 0034, and thus the amendment does not constitute new matter.

Claim 6 has been amended to adjust its dependency in view of the cancelation of claim 5, and thus does not add new matter.

Claim 12 has been amended to correct a minor typographical oversight, and thus does not add new matter.

Claim 23 has been amended in a manner supported at least by paragraph 0034, and thus does not constitute new matter.

The amendments to claims 20-22 are supported at least by paragraph 0021, and thus do not constitute new matter.

The amendment to the specification corrects only a minor typographical oversight, and does not add new matter.

Conclusion

For all of the foregoing reasons, applicants submit that this case is in condition for allowance.

Date: April 20, 2007

/Steven J. Rocci/
Steven J. Rocci
Registration No. 30,489

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439